Grandstream Networks, Inc.

Captive Portal

Basic Configuration & Customization

Table of Content

SUPPORTED DEVICES 4

INTRODUCTION 5

CAPTIVE PORTAL SETTINGS 6

Policy Configuration Page 6

Landing Page Redirection *8*

Pre-Authentication Rules *8*

Post-Authentication Rules *8*

Files Configuration Page 9

Clients Page 11

CAPTIVE PORTAL BASIC CONFIGURATION STEPS 12

Scenario Overview 12

Custom Portal Page 12

HTML code *12*

Variables *13*

Configure Captive Portal Settings 14

Upload Custom HTML Portal Page *14*

Configure Captive Portal Settings *14*

Table of Figures

Figure 1: General Architecture 5
Figure 2: Captive Portal web GUI menu 6
Figure 3: portal_default.html page 9
Figure 4: Files Web Page 10
Figure 5: Client Web Page 11
Figure 6: File Upload window 14
Figure 7: Captive Portal Sample Configuration 15
Figure 8: Enable Captive Portal on Network Groups 16
Figure 9: Portal Page 16

Table of Tables

Table 1: Supported Devices 4
Table 2: Policy Configuration Page 7

SUPPORTED DEVICES

Following table shows Grandstream devices supporting Captive Portal feature:

Table 1: Supported Devices

Model	Supported	Firmware
GWN7610	Yes	1.0.3.19 or higher
GWN7600	Yes	1.0.3.19 or higher
GWN7000	Yes	1.0.2.75 or higher

INTRODUCTION

Captive Portal feature on GWN76XX Access Points and GWN7000 router allows to define a Portal Web Page that will be displayed on WiFi clients' browsers when attempting to access the Internet.

Once connected to GWN76XX AP, WiFi clients will be forced to view and interact with that landing page before Internet access is granted.

Captive portal can be used in different environments including airports, hotels, coffee shops, business centers and others offering free WiFi hotspots for Internet users.

This guide describes how to setup a basic captive portal feature on the GWN76XX series.

The following figure illustrates an example of the landing page feature.

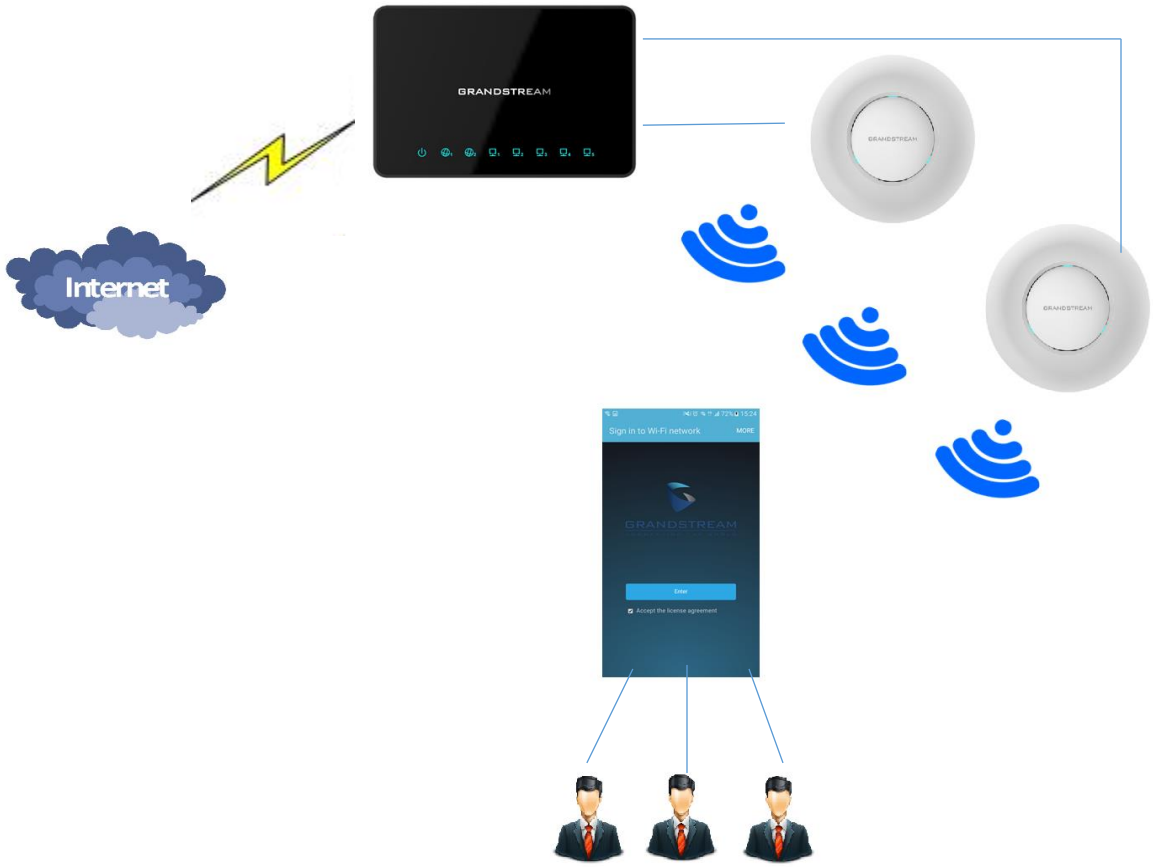


Figure 1: General Architecture

CAPTIVE PORTAL SETTINGS

The Captive Portal feature can be configured from the GWN76XX/GWN7000 web page, by navigating to "**Captive Portal**".

The page contains three tabs: **Policy**, **Files** and **Clients**.

- **Policy Tab**: In this page, users can configure multiple portal policies which then can be assigned to specifc network groups under the menu "**Network Groups**". (For example having non-authentication based portal for temporary guests and setting up an authentication based portal policy for the internal staff).
- **Files Tab**: Under this tab, users could download and upload customized portal landing page to display to the users when they try to connect over the WiFi.
- **Clients Tab**: This tab lists the authenticated clients MAC addresses.

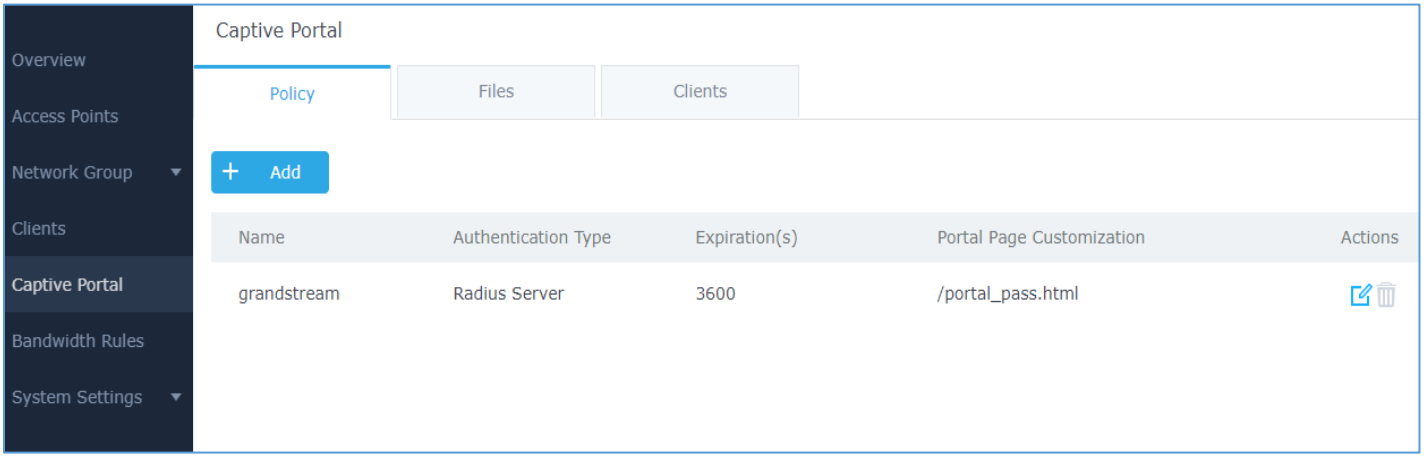


Figure 2: Captive Portal web GUI menu

Policy Configuration Page

The Policy configuration allows users to configure and customize different captive portal policies which then can be selected on network group configuration page, giving the admin the ability to set different captive portals for each network group.

The following table describes the settings used for Basic Configuration of the Captive Portal feature:

Table 2: Policy Configuration Page

Field	Description
Name	Enter a name to identify the created policy (ex: Guest Portal).
Expiration	Enter the expiration time for the landing page, this field must contain an integer between 60 or 604800 in minutes. If this field is set to 0 the landing page will never expire.
Authentication Type	Three types of authentication are available: • **No Authentication:** when choosing this option, the landing page feature will not provide any type of authentication, instead it will prompt users to accept the license agreement to gain access to internet. In this guide, we will use this option for basic configuration without authentication. • **RADIUS Server:** Choosing this option will allow users to set a RADIUS server to authenticate connecting clients. • **Third Authentication:** Choosing this option will allow users to log in using WeChat or Facebook.
Portal Page Customization	This option allows users to choose the landing page that will be shown once a client tries to connect to the Internet, three pages are available: • **Portal Default:** This page is used when no authentication is specified, users will have only to accept license agreement to gain access to internet. In this guide, we will use this option. • **Portal Pass:** This option provides authentication textbox when using RADIUS authentication mode to enter username and password stored in RADIUS database. • **Third Auth:** Choose this page when using authentication via WeChat or Facebook.
Landing Page	Select where to redirect authenticated clients. • **Redirect to the original URL:** Sends the authenticated client to the original requested URL. • **Redirect External Page:** Enter URL that you want to promote to connected clients (ex: company's website).
Redirect External Page URL	When setting the landing page to (Redirect External Page), enter the URL where to redirect authenticated clients.
Enable HTTPS	Check this box to enable captive portal over HTTPS.
Pre-Authentication Rules	From this menu, users can set matching rules to allow certain types of traffic before authentication happens or simply allow the traffic for non-authenticated end points.

Post Authentication Rules	This can be used to block certain type of traffic to authenticated clients. If used, only defined traffic will be blocked and everything else is allowed by default. (Ex: Settings a rule that matches HTTP will ban all authenticated clients to not access web server that are based on HTTP).

Landing Page Redirection

This feature can be configured using the option “Redirect External Page URL” under the policy settings, and could be useful in the case the network admin wants to force all connected guest clients to be redirected to a certain URL (ex: company’s website) for promotion and advertisement purposes.

Note: Supported on GWN7600 Access Points only.

Pre-Authentication Rules

Using this option, users can set rules to match traffic that will be allowed for connected WiFi users before authentication process. This can be needed for example to setup Facebook authentication where some traffic should be allowed to Facebook server(s) to process the user’s authentication. Or simply to be used to allow some type of traffic for unauthenticated users.

Note: Supported on GWN7600 Access Points only.

Post-Authentication Rules

On the other hand, post authentication rules are used to match traffic that will be banned for WiFi clients after authentication. As an example, if you want to disallow connected WiFi clients to issue Telnet or SSH traffic after authentication then you can set post authentication rules to match that traffic and once a connected client passes the authentication process they will be banned from issuing telnet and SSH connections.

Note: Supported on GWN7600 Access Points only.

Files Configuration Page

Files configuration page allows to view and upload HTML pages and related files (images…).

The captive portal uses **portal_default.html** as default portal page, WiFi clients will be redirected to this page before accessing Internet, but you could upload your own custom page and select it as default portal page or customize the existing one.

The following figure shows the display of portal_default.html page:

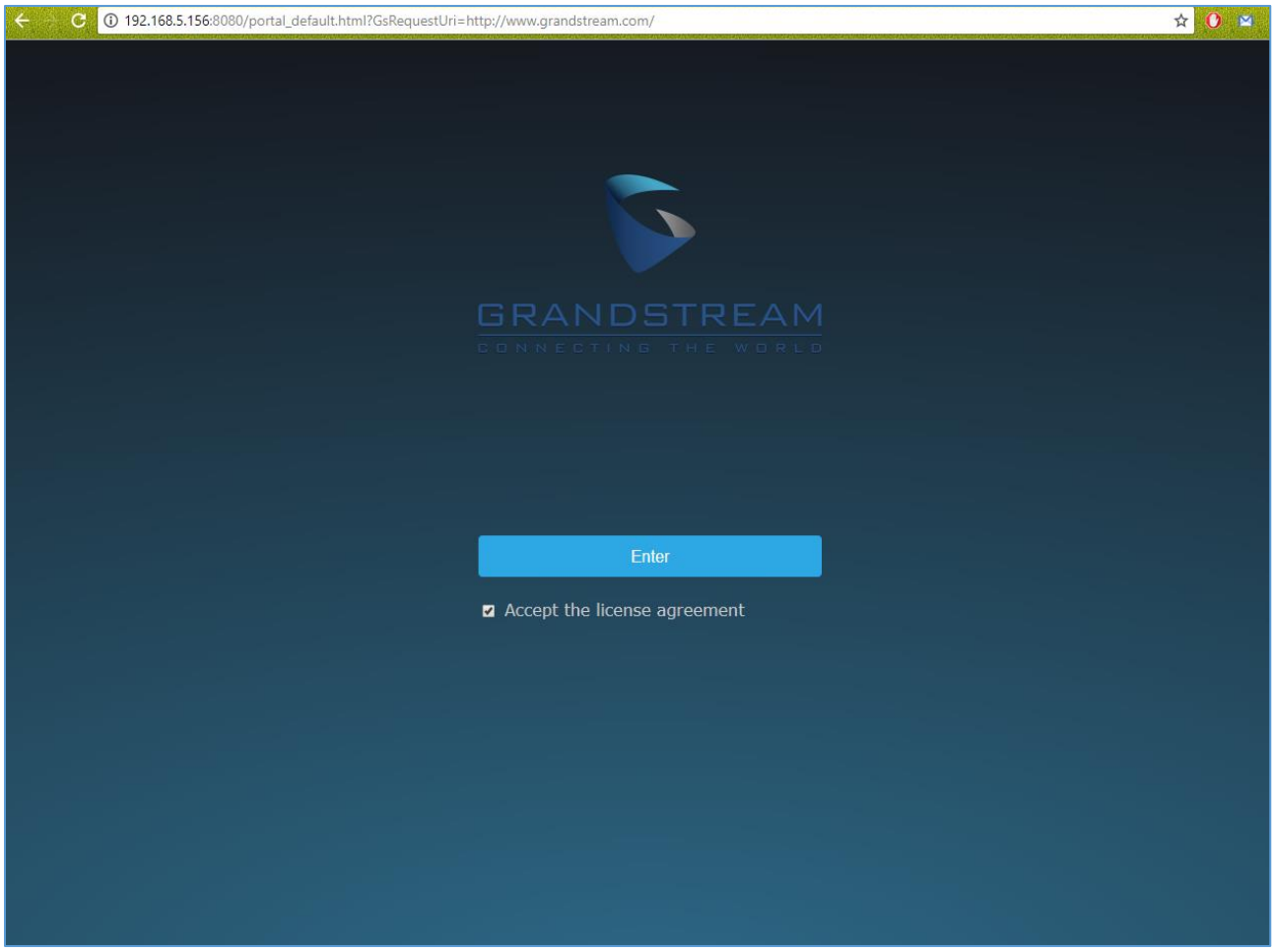


Figure 3: portal_default.html page

The following figure shows default files used for Captive Portal in GWN Access point and/or GWN router, please note that user could customize these files to reflect enterprise logo and policy.

This option will be discussed in more details with sample configuration on the next sections of customizing captive porta.

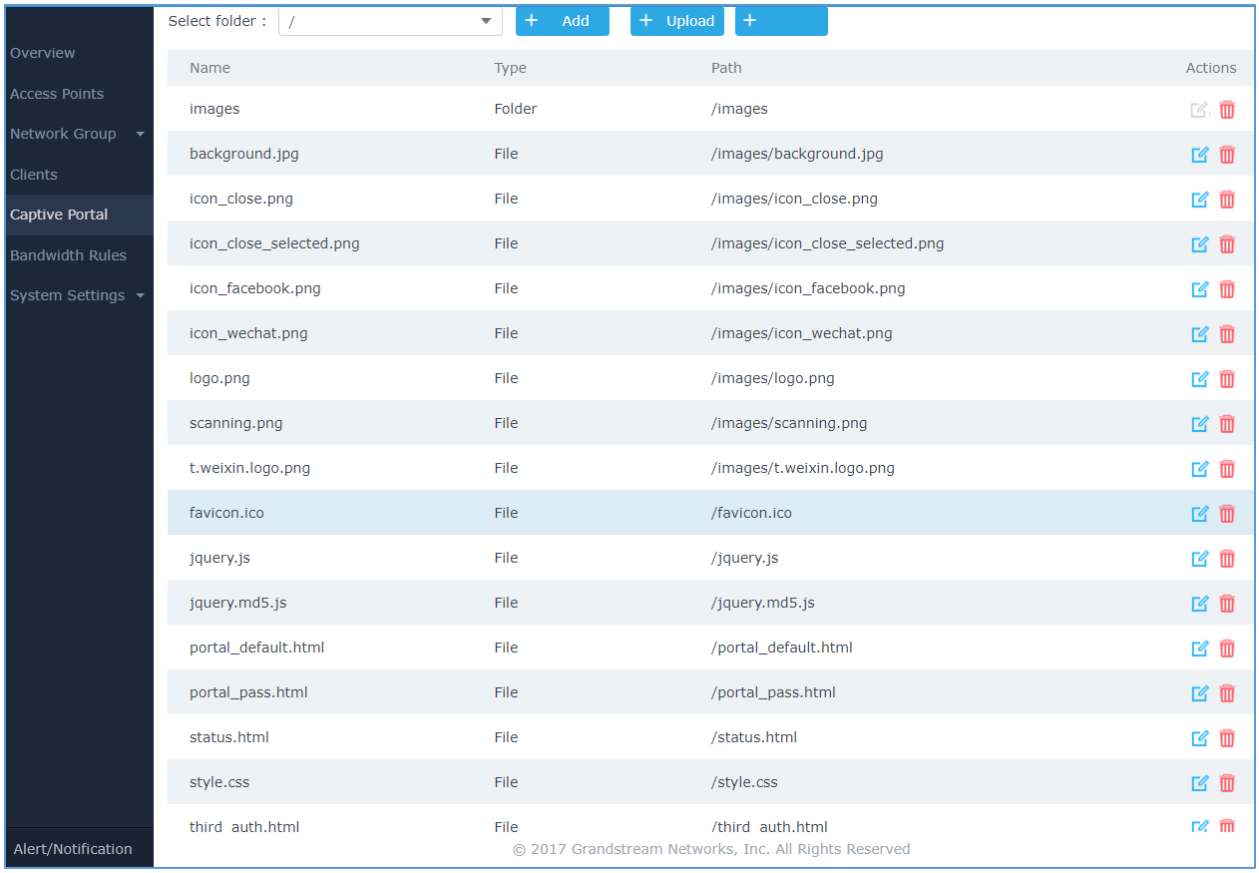
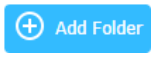
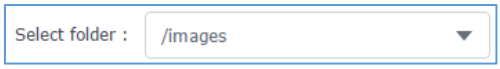


Figure 4: Files Web Page

- Click  to upload a new web page.
- Click  to add a new folder.
- Click  to upload files to the selected folder.
- Folder can be selected from the dropdown list  .

Landing page can be customized depending on customer's needs. Please refer to [***CAPTIVE PORTAL***] for more details.

Clients Page

For Information Purposes Clients page lists MAC addresses of authenticated devices using captive portal. As we can see on the below figure, two WiFi clients have been authenticated and granted internet access from the GWN7610 access points:

- ✓ Client 1 → ***E8:DE:27:0B:C1:E7***
- ✓ Client 2 → ***DC:09:4C:A4:38:BE***

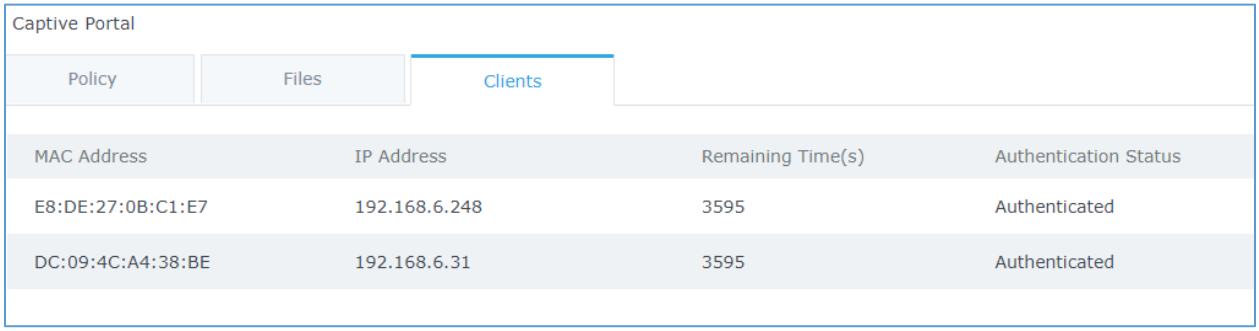


Figure 5: Client Web Page

CAPTIVE PORTAL BASIC CONFIGURATION STEPS

In this section, we will provide all steps needed to use Captive Portal with customized settings.

Scenario Overview

We consider that ABC company has deployed GWN76XX Access Points and wants to configure Captive Portal.

Below are ABC company requirements:

- The default landing page should be customized with ABC company logo and “Terms of Use”.
- Users need to read and accept “Terms and Conditions” to get Internet access.
- After accepting the terms of use, the clients should be redirected to company ABC website.
- All clients should be re-authenticated after 1 hour.

Custom Portal Page

HTML code

The following is an example of customized portal html code that reflect company ABC terms:

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<meta charset="utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<link rel='shortcut icon' href='$imagesdir/abc.png' type='image/x-icon' />
<title>$gatewayname Entry</title>
<style>

Body { background-color:white;
color:black;
margin-left: 5%;
margin-right: 5%;
text-align: left; }
Img { width: 100%;
max-width: 500px;
margin-left: 5%;
margin-right: 5%; }
  .bordered {
    width: 800px;
    height: 200px;
    padding: 5px;
    border: 2px solid #AAAAAA;
       overflow: auto;
       text-align: justify;
       margin-left: 15%;
    margin-right: 15%;

  }
input [type=submit] {
color:black;
```

```
margin-left: 0%;
margin-right: 5%;
text-align:left;
font-size: 1.0em;
line-height: 2.5em;
font-weight: bold;
border: 1px solid; }
</style>
</head>
<body>
<b>$gatewayname Hotspot</b>
<div style="text-align: center;">
<br> <br> <b>
<img src="$imagesdir/abc.png" alt="Splash image" align="center">

<br> <br>
<span style="color:blue; font-style:normal; font-size: 300%;" align="center"> Welcome!
</span>
</b> <br> <br> <br>
<b>For access to the Internet, please read license and click on "Accept Terms"</b>
<br> <br>
<div class="bordered">
<p>Terms of Use conditions</p>
</div>
</br>
<form method='get' action='$authaction'>
<input type='hidden' name='tok' value='$tok'>
<input type='hidden' name='redir' value='$redir'>
<input type='submit' value='I have read and accept "Terms of Use"'>
</form>
</div>
</body>
</html>
```

Variables

"**$tok**", "**$redir**" and "**$authaction**" variables can be used with GET-method in HTML form to communicate with the server.

$tok	Token sent by the device trying to connect to the AP.
$authaction	URL of the gateway.
$redir	URL user typed initially. Once connected successfully users will be redirected to that URL.

Configure Captive Portal Settings

Upload Custom HTML Portal Page

To upload custom portal page, follow below steps:

1. Access GWN76xx Web interface under the menu **Captive Portal**.
2. Go to **Files** tab.
    a. Click on Upload button.
    b. In “File upload” popup window, press “Choose File” to browse customized portal page file and press OK.

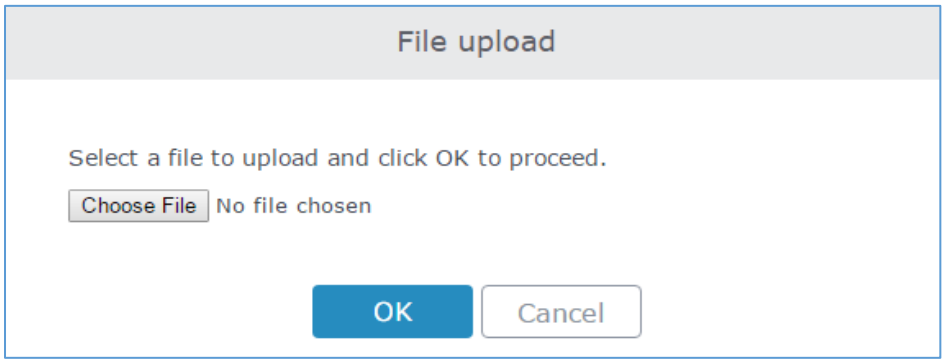


Figure 6: File Upload window

    c. In “Select Folder” drop-down list, select “Images”.
    d. Press 

button to upload related images (in this example, we need to upload “abc.png” file which is ABC company logo image).

Configure Captive Portal Settings

To configure captive portal with ABC company requirements, follow below steps:

1. Access GWN76xx Web interface under **Captive Portal**.
2. Go to **Policy** tab.
3. Click Add to add a new policy that meets company ABC requirements.

Following screenshot shows the configuration of the new added policy:

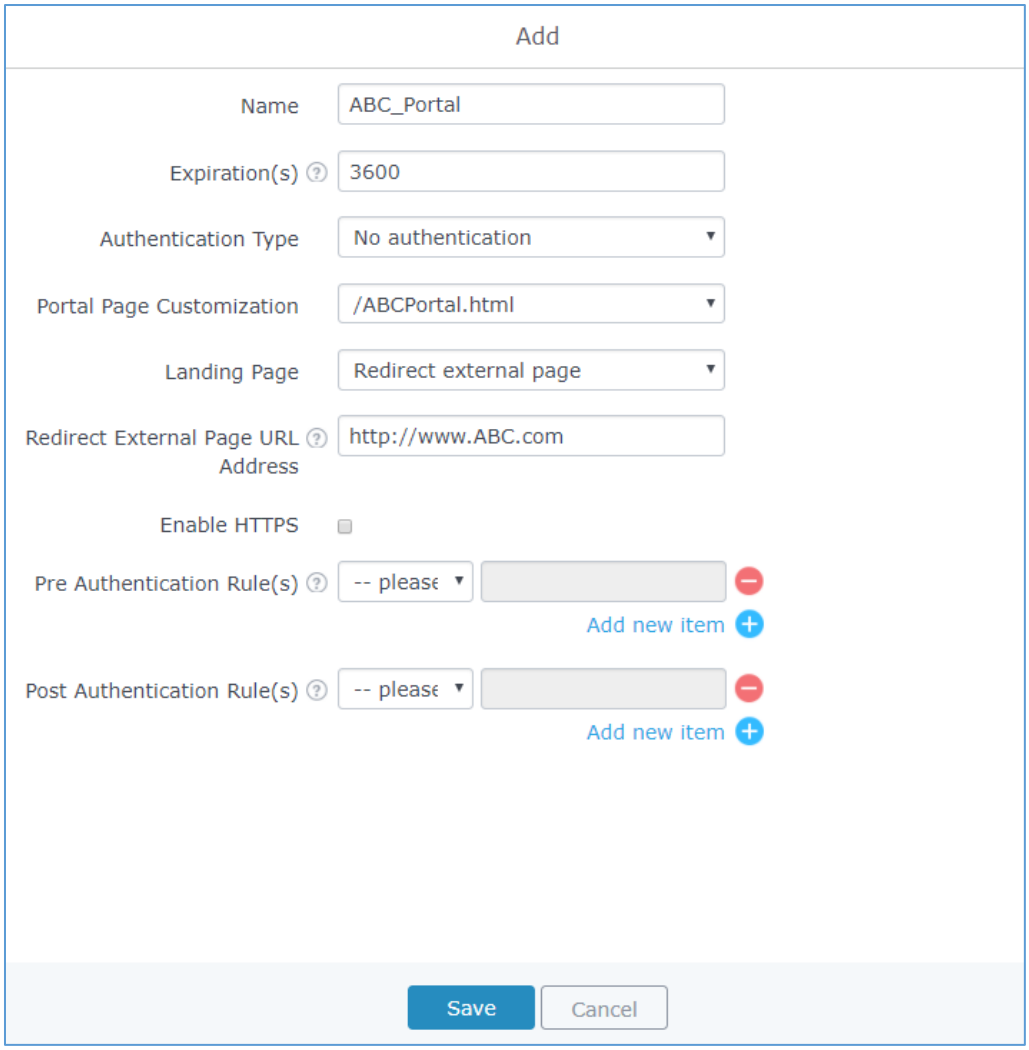


Figure 7: Captive Portal Sample Configuration

4. Press Save then Apply.
5. Go to **Network Group** menu and edit the desired group where the portal should be enabled, this can be done under WiFi settings tab as shown on the following figure.

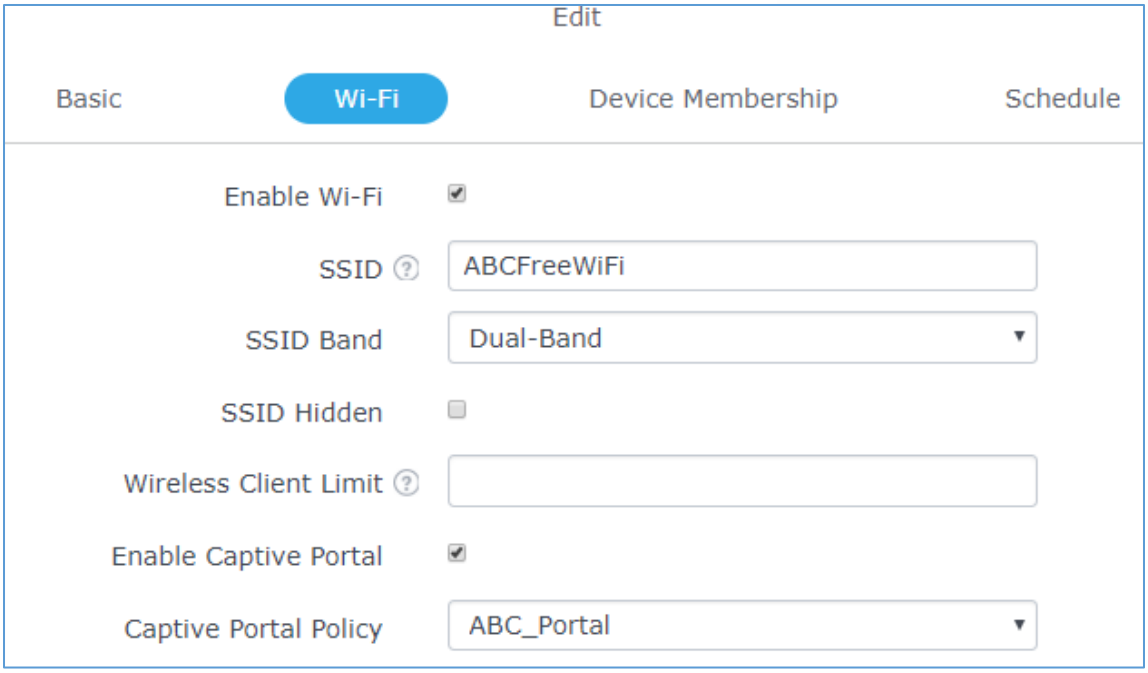


Figure 8: Enable Captive Portal on Network Groups

6. At this stage, WiFi clients trying to access Internet via GWN76xx access point will get customized portal page first, they will need next to accept the terms of use to get Internet access.

Figure 9: Portal Page